We claim:

1. A system for secure ticketing in a communications device, comprising:

a mobile equipment that includes a first storage device;

a security element that includes a second storage device;

at least one third-party device; and

a processor in communication with said first storage device, said second storage device and said third-party device configured to:

authenticate said security element;

created and initiate at least one counter stored in said second storage device in said secure element;

receive at least one electronic ticket from said third-party device and storing said at least one electronic ticket in said first storage device;

redeem said at least one electronic ticket stored in said first storage device with said at least one third-party device; and

update a counter value for the counter in said second storage device to correspond to the redemption of said electronic ticket with said third-party device.

2. The system of claim 1, wherein said counter stored in said second storage device is a monotonically increasing counter comprising a unique identifier and an associated current value corresponding to each of the stored electronic tickets.

3. The system of claim 1, wherein said counter stored in said second storage device is a monotonically decreasing counter comprising a unique identifier and an associated current value corresponding to each of the stored electronic tickets.

4. The system of claim 1, wherein said at least one electronic ticket sent by said at least one third-party device includes the counter value for the counter in said second storage device.

5. The system of claim 4, wherein the counter value is determined by the third-party device to correspond to a number of uses of a service provided by a third-party.

6. The system of claim 1, wherein said first storage device is an internal memory device in said communications device.

7. The system of claim 1, wherein said second storage device is a tamper-resistant memory device removably received by said communications device.

8. The system of claim 7, wherein said second storage device is an electronic card that is received by the communications device.

9. The system of claim 1 wherein said processor is a central processor in said communications device.

10. The system of claim 1, wherein the communication between said mobile equipment, security element and third-party device comprises the execution of a plurality of protocols using an operating system of the communications device.

11. The system of claim 10, wherein said plurality of protocols comprise a request and store ticket protocol, use ticket protocol, and check ticket protocol.

12. The system of claim 1, wherein said second storage device further comprises a manufacturer's certificate and a signature key pair.

13. The system of claim 1, wherein said second storage device further comprises an encryption key pair.

14. The system of claim 1, wherein said at least one third-party device further comprises an encryption key pair and a signature key pair.

15. The system of claim 1, wherein said at least one third-party device comprises at a ticket issuing device, a ticket collecting device and a checking device.

16. The system of claim 1, wherein said at least one third-party comprises a plurality of ticket collecting devices.

17. The system of claim 1, wherein the communications device comprises a cellular telephone, a satellite telephone, a personal digital assistant, a personal trusted device or a bluetooth device.

18. The method of secure ticketing in a communications device, comprising:

authenticating a security element;

creating and initiating at least one counter in said security element;

requesting at least one electronic ticket from at least one third-party device;

storing said at least one electronic ticket received from said at least one third-party storage device in a storage device of said communications device;

redeeming said at least one electronic ticket stored in said storage device with said at least one third-party device; and

updating a counter value in said security element to correspond to the redemption of said electronic ticket with at least one third-party device.

19. The method of claim 18, wherein said electronic ticket sent by said at least one third-party device includes the counter value for the counter in said security element.

20. The method of claims 19, wherein the counter value is determined by said at least one third-party device to correspond to a number of uses of a service provided by a third-party.

21. The method of claim 18, wherein said storage device is an internal memory device in the communications device.

22. The method of claim 18, wherein said security element comprises a tamper-resistant, read-write memory device removably received by said communications device.

23. The method of claim 18, further comprising storing a public key of said secured element in at least one third-party device.

24. The method of claim 18, further comprising storing a master key in said at least one third-party device.

25. The method of claim 18, wherein the communications device is a cellular telephone, a satellite telephone, a personal digital assistant, a personal trusted device or a bluetooth device.

26. The method of claim 18, wherein said at least one third-party comprises at a ticket issuing device, a ticket collecting device and a checking device.

27. A computer program product for secured ticketing in a communications device, comprising:

a computer readable medium;

program code in said computer readable medium for authenticating a security element;

program code in said computer readable medium for initiating at least one counter in said security element;

program code in said computer readable medium for requesting at least one electronic ticket from at least one third-party device;

program code in said computer-readable medium for storing said electronic ticket from said at least one third-party device in a storage device of said communications device;

program code in said computer-readable medium for redeeming said at least one electronic ticket stored in said storage device with at least one third-party device; and

program code in said computer readable for updating a counter value in said security element to correspond to redemption of said at least one electronic ticket with at least one third-party device.

28. A method of requesting, creating, and storing a ticket for secure ticketing in a system comprising a mobile equipment having a first storage device, a secure element having a security element comprising a second storage device with a certificate and a pair of encryption keys, and at least one third-party device having a cryptographic master public key and configured to issue tickets, the method comprising:

authenticating the said security element;

creating at least one counter in said security element;

requesting at least one ticket from said third-party device;

creating at least one ticket by the said third-party device;

receiving at least one ticket from the said third-party device, and

storing the said at least one ticket received in the first storage device.

29. The method of claim 28, wherein said authenticating the security element comprises:

said mobile equipment sending a request to the security element for a certificate of authenticity;

said security element sending as a response the certificate;

said mobile equipment receiving said certificate; and

said mobile equipment verifying the compliance of the received certificate.

30. The method of claim 28, wherein said creating at least one counter comprises:

said mobile equipment sending a request to create a counter in the security element;

said security element creating a counter by giving a unique counter ID, and initializing the counter to zero; and

said security element sending the created counter ID to said mobile equipment.

31. The method of claim 28, wherein said requesting at least one ticket comprises:

said mobile equipment sending to the said third-party device:

a newly created counter ID received from the said security element;

a certificate of the security element; and

a public key of the security element.

32. The method of claim 28, wherein creating at least one ticket comprises:

the third party receiving from the mobile equipment a counter ID, a certificate of the security element, and a public key of the security element;

the third party creating at least one ticket by forming a signature on authenticator data consisting of the received counter ID, said public key of the third party, a number representing the number of allowed uses for the ticket, and additional information;

the third party generating a message authentication key associated with the received counter ID; and

the third party creating an encryption key by encrypting with the said public key of the security element the received counter ID and the generated message authentication key.

33. The method of claim 28, wherein receiving at least one ticket comprises:

said mobile equipment receiving at least one ticket created by the said third-party device, the ticket being a signature on authenticator data consisting of the received counter ID, said third party public key, a number representing the number of allowed uses for the ticket, and additional information; and said mobile equipment receiving an encryption key created by the said third-party device by encrypting with the public key of the security element the received counter ID and the associated message authentication key.

34. A method of claim 28, wherein said storing at least one ticket comprises:

said mobile equipment storing in the said first storage device the received at least one ticket created by the said third-party device, the ticket being a signature on authenticator data consisting of the received counter ID, said third party public key, a number representing the number of allowed uses for the ticket, and additional information;

said mobile equipment forwarding to the said security element a received encryption key created by the said third-party device by encrypting with the public key of the security element the received counter ID and a message authentication key generated by the third-party device and associated with the counter ID;

said security element recovering the message authentication key from the received encryption key;

said security element storing the message authentication key and associating it with the counter ID; and

said security element sending an acknowledgement to the mobile equipment.

35. A method of using a ticket in a system for secure ticketing comprising

a mobile equipment having a first storage device with a ticket stored therein,

a secure element having a security element comprising a second storage device having a certificate, a pair of encryption keys, and at least one counter related to the stored ticket, the counter having an unique counter ID, a counter value, and a message authentication key, and

at least one third-party device having a cryptographic master public key, the third-party configured to redeem tickets, the ticket being a signature on authenticator data consisting of a counter ID, said public key of the third-party, a number representing the number of allowed uses for the ticket, and additional information, the method comprising:

said mobile equipment sending the stored ticket to the said third-party device for redeeming;

said third-party device checking the validity of the received ticket;

said third party sending a challenge to the said mobile equipment, if the ticket is deemed valid;

said mobile equipment invoking counter update in said security element for the counter related to the ticket to be redeemed by sending the corresponding counter ID and said received challenge;

said security element updating the said counter with a value specified by the third-party device;

said security element generating an authorization token being a message authentication code computed by using the message authentication key stored in the counter;

said security element sending the generated authorization token to the said mobile equipment;

said mobile equipment forwarding the received authorization token to the said third-party device;

said third-party device verifying the received authorization token by using the key in the received ticket; and

said third-party device checking the current value of counter against the number of allowed uses in the ticket and sending a message to the mobile equipment corresponding the result of the check.

36. A method of claim 35, wherein the checking of the validity of the received ticket comprises verification of the signature on the ticket.

37. A method of claim 35, wherein the checking of the validity of the received ticket further comprises validity check of the additional information in the ticket.

38. A method of claim 35, wherein the message corresponding to the result of the check for counter value is a validated ticket being a signature on authenticator data consisting the said counter ID, said public key, and said current counter value all taken from the received authorization token, and additional information.

39. A method of claim 35, further comprising storing the received validated ticket in the first storage device.

40. A method of claim 35, further comprising:

said mobile equipment receiving a message as a result of the of the check for counter value showing that the ticket is fully used;

said mobile equipment sending a request to the said security element to delete the said counter; and

said security element returning the result of the delete counter request as a response.

41. A method of claim 35, wherein the ticket is a multi-use ticket, the method comprising:

sending the stored ticket to the third-party device with sending also the stored validated tickets to the third-party device and using the additional information in the validated tickets for access control.

42. A method of checking a ticket in a system for secure ticketing comprising

a mobile equipment having a first storage device with a ticket stored therein,

a secure element having a security element comprising a second storage device having a certificate, a pair of encryption keys, and at least one counter related to the stored ticket, the counter having an unique counter ID, a counter value, and a message authentication key, and at least one third-party device having a cryptographic master public key, the third-party configured to check tickets, the ticket being a signature on authenticator data consisting of a counter ID, a public key of the third-party, a number representing the number of allowed uses for the ticket, and additional information, the method comprising:

said mobile equipment sending the stored ticket to the said third-party device for checking;

said third-party device checking the validity of the received ticket;

said third-party sending a challenge to the said mobile equipment;

said mobile equipment invoking a read counter in said security element for the counter related to the ticket to be checked by sending the corresponding counter ID and said received challenge;

said security element generating an authorization token being a message authentication code computed by using the message authentication key stored in the counter;

said security element sending the generated authorization token to the said mobile equipment;

said mobile equipment forwarding the received authorization token to the said third-party device; and

said third-party device verifying the received authorization token by using the key in the received ticket and sending a message to the said mobile device indicating the result of the verification.

43. A security construction for a ticket system comprising:

an equipment having a first storage device,

a secure element linked to the first storage device, the security element comprising a second storage device having a pair of encryption keys and a certificate, and at least one counter in said security element comprising a unique counter ID and a counter value;

at least one ticket stored at least partly in the first storage device having information about one of the encryption keys of the security element, counter ID; and

allowed use information operationally communicated with the security element to update counter value in the respective counter identified by the counter ID in the security element.

44. A method of requesting, creating, and storing a ticket for secure ticketing in a system comprising a mobile equipment having a first storage device, a secure element having a security element comprising a second storage device having a certificate and a pair of encryption keys, and at least one third-party device configured to issue tickets,
the method comprising:

authenticating the said security element;

creating at least one counter in said security element;

requesting at least one ticket from said third-party device;

creating at least one ticket by the said third-party device;

receiving at least one ticket from the said third-party device, and

storing the said at least one ticket received in the first storage device.

45. A method of claim 44, wherein said authenticating the security element comprises the steps of:

said mobile equipment sending a request to the security element for a certificate of authenticity;

said security element sending as a response the certificate;

said mobile equipment receiving said certificate; and

said mobile equipment verifying the compliance of the received certificate.

46. A method of claim 44, wherein creating at least one counter comprises:

said mobile equipment sending a request to create a counter in the security element;

said security element creating a counter by giving a unique counter ID and initializing the counter to zero; and

said security element sending the created counter ID to said mobile equipment.

47. A method of claim 44, wherein said requesting at least one ticket comprises:

said mobile equipment sending to the said third-party device, a newly created counter ID received from the said security element, a certificate of the security element, and a public key of the security element

48. A method of claim 44 wherein said creating at least one ticket by the third-party comprises:

receiving from the mobile equipment a counter ID, a certificate of the security element and a public key of the security element;

creating at least one ticket by forming a signature on authenticator data consisting of the received counter ID, received public key, a number representing the number of allowed uses for the ticket, and additional information.

49. A method of claim 44, wherein receiving at least one ticket comprises

said mobile equipment receiving at least one ticket created by the said third-party device, the ticket being a signature on authenticator data consisting of the received counter ID, received public key, a number representing the number of allowed uses for the ticket, and additional information.

50. A method of claim 44, wherein said storing at least one ticket comprises:

storing in the said first storage device the received at least one ticket created by the said third-party device, the ticket being a signature on authenticator data consisting of the received counter ID, received public key, a number representing the number of allowed uses for the ticket, and additional information.

51. A method of using a ticket in a system for secure ticketing comprising a mobile equipment having a first storage device with a ticket stored therein, a secure element having a security element comprising a second storage device having a certificate, a pair of encryption keys, and at least one counter related to the stored ticket; and at least one third-

party device configured to redeem tickets, the ticket being a signature on authenticator data consisting of a counter ID, a public key of the secure element, a number representing the number of allowed uses for the ticket, and additional information, the method comprising:

said mobile equipment sending the stored ticket to the said third-party device for redeeming;

said third-party device checking the validity of the received ticket;

said third party sending a challenge to the said mobile equipment, if the ticket is deemed valid;

said mobile equipment invoking counter update in said security element for the counter related to the ticket to be redeemed by sending the corresponding counter ID and said received challenge;

said security element updating the said counter with a value specified by the third-party device;

said security element generating an authorization token being a signature on authenticator data comprising the said counter ID, current value of the counter, and the public key of the security element;

said security element sending the generated authorization token to the said mobile equipment;

said mobile equipment forwarding the received authorization token to the said third-party device;

said third-party device verifying the received authorization token by using the key in the received

ticket; and

said third-party device checking the current value of counter against the number of allowed uses in the ticket and sending a message to the mobile equipment corresponding the result of the check.

52. A method of claim 51, wherein the checking of the validity of the received ticket comprises verification of the signature on the ticket.

53. A method of claim 51, wherein the checking of the validity of the received ticket further comprises validity check of the additional information in the ticket.

54. A method of claim 51, wherein the message corresponding to the result of the check for counter value is a validated ticket being a signature on authenticator data consisting the said counter ID, said public key, and said current counter value all taken from the received authorization token, and additional information.

55. A method of claim 51, further comprising storing the received validated ticket in the first storage device.

56. A method of claim 51, further comprising:

said mobile equipment receiving a message as a result of the of the check for counter value showing that the ticket is fully used;

said mobile equipment sending a request to the said security element to delete the said counter; and

said security element returning the result of the delete counter request as a response.

57. A method of claim 51, wherein the ticket is a multi-use ticket, and the method comprising:

sending the stored ticket to the third-party device with sending also the stored validated tickets to the third-party device and using the additional information in the validated tickets for access control.

58. A method of checking a ticket in a system for secure ticketing comprising

a mobile equipment having a first storage device with a ticket stored therein, a secure element having a security element comprising a second storage device having a certificate, a pair of encryption keys, and at least one counter related to the stored ticket; and at least one third-party device configured to check tickets, the ticket being a signature on authenticator data consisting of a counter ID, a public key of the secure element, a number representing the number of allowed uses for the ticket, and additional information, the method comprising:

said mobile equipment sending the stored ticket to the said third-party device for checking;

said third-party device checking the validity of the received ticket;

said third-party sending a challenge to the said mobile equipment;

said mobile equipment invoking a read counter in said security element for the counter related to the ticket to be checked by sending the corresponding counter ID and said received challenge;

said security element generating an authorization token being a signature on authenticator data comprising the said counter ID, current value of the counter, and the public key of the security element;

said security element sending the generated authorization token to the said mobile equipment;

said mobile equipment forwarding the received authorization token to the said third-party device; and

said third-party device verifying the received authorization token by using the key in the received ticket and sending a message to the said mobile device indicating the result of the verification.